Remarks

Reconsideration of this Application is respectfully requested.

Applicants respectfully request admission of the foregoing amendment to place the application in condition for allowance by traversing the rejections under 35 U.S.C. § 103.

Upon entry of the foregoing amendment, claims 1, 2, 4-18, 20-36, and 38-56 are pending in the application, with claims 1, 11, 20, 24, 31, and 40 being the independent claims. Claims 1, 2, 4-14, 18, 20-34, 38, 40-43, 46, 47, 51, 53, 54, and 55 are sought to be amended. Claims 19 and 37 are sought to be canceled without prejudice to or disclaimer of the subject matter therein. These changes are believed to introduce no new matter, and their entry is respectfully requested.

Based on the above amendment and the following remarks, Applicants respectfully request that the Examiner reconsider all outstanding rejections and that they be withdrawn.

Rejections Under 35 U.S.C. § 103

Hirano in View of Laczko

Claims 1, 2, 4-10, 20-31, 33-42, 45-51, and 53-56 were rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over U.S. Patent No. 7,046,807 issued to Hirano *et al.* ("Hirano") in view of U.S. Patent No. 6,711,683 issued to Laczko, Sr *et al.* ("Laczko").

Regarding claim 37, Applicants have canceled this claim without prejudice to or disclaimer of the subject matter therein, thereby rendering this rejection moot.

Regarding claims 1, 2, 4-10, 20-31, 33-36, 38-42, 45-51, and 53-56, Applicants respectfully traverse these rejections.

Independent claim 1 recites (emphasis added):

> A computer implemented method for securing a file, the method comprising:
> determining whether the file ***stored in a file system*** and being accessed is secured;
> if the file is determined to be secured, activating a cipher module and loading the file ***from the file system*** through the cipher module into an application; and
> if the file is determined to be non-secured, loading the file ***from the file system*** into the application without activating the cipher module.

Each of independent claims 20 and 24 recites similar features. Neither Hirano nor Laczko, alone or in combination, discloses, teaches, or suggests a method for securing a file in which a determination of whether a file is secured is performed when the file is stored in a file system ***before*** the file is loaded into an application. Hirano, at column 6, lines 24-56, recites (emphasis added):

> FIG. **1** shows the structure of an outline of the present invention.
> A contents supplier **1** is a copyright holder of the digital content and supplies to a content administrator **2** digital content **11** to be administered.
> ***The contents manager 2 encrypts the digital content 11 supplied from the contents supplier 1*** for administration, manages a contents key used as a encryption key for encrypting and manages the user information of users that use the digital content **11**.
> The contents user **3** transmits the user information **14** to the contents manager 2 in the case where the contents user **3** would like to employ the digital content that the contents manager **2** manages.
> The contents manager **2** manages the user information **14** transmitted from the contents user **3**, produces consent information **13** on the basis of the user information **14** and synthetic data **12** including ***a real data section 15 that encrypts the digital content*** and the consent information **13** to the contents user **3**.
> In this situation, the contents manager **2** produces the header data section **16** by using symbol information symbolized so as to visually and auditorily recognize the attribute of the digital content **11**. The contents manager **2** encrypts the contents key used when encrypting the digital content **11** by the user information **14** to produce the consent information **13**, and

> produces the consent information added header data section where the consent information is embedded in the header data section **16** as an electronic watermark. In addition, ***the contents manager 2 synthesizes the real data section 15 that encrypts the digital content and the consent information added header data section and transmits it to the contents user 3.***

In other words, in Hirano, the accessed file is not secured when stored at the contents supplier, but rather is encrypted by the contents manager in the process of being accessed by the contents user. Laczko does not overcome this deficiency. Therefore, each of independent claims 1, 20, and 24 is patentable over Hirano in view of Laczko.

Independent claim 31 recites (emphasis added):

> A computer readable storage medium having computer program code recorded thereon, that when executed by a processor, causes the processor to secure a file by a method, comprising:
>
> maintaining a file key in a temporary memory space;
>
> encrypting the file with the file key in a cipher module to produce an encrypted file, wherein the file has been opened with an application and the cipher module operates transparently as far as a user executing the application is concerned; and
>
> storing, in a storage space, a secured file including the encrypted file and a header, wherein the header includes or points to security information including the file key, wherein the security information further includes ***access rules of how*** and by whom ***the file is to be accessed.***

Independent claim 40 recites similar features. Neither Hirano nor Laczko, alone or in combination, discloses, teaches, or suggests a method to secure a file that uses access rules of ***how*** the file is to be accessed. Therefore, each of independent claims 31 and 40 is patentable over Hirano in view of Laczko.

Because each of claims 2, 4-10, 21-23, 25-30, 33-36, 38, 39, 41, 42, 45-51, and 53-56 depends upon claims 1, 20, 24, 31, or 40 and because of the additional distinctive features of each of claims 2, 4-10, 21-23, 25-30, 33-36, 38, 39, 41, 42, 45-51, and 53-56, each of these claims is also patentable over Hirano in view of Laczko.

Accordingly, Applicants respectfully request that the Examiner reconsider and remove the rejections of claims 1, 2, 4-10, 20-31, 33-36, 38-42, 45-51, and 53-56 under 35 U.S.C. § 103(a).

Hirano in View of Novak

Claims 11-19, 32, 43, 44 and 52 were rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Hirano in view of U.S. Patent No. 6,865,555 issued to Novak ("Novak").

Regarding claim 19, Applicants have canceled this claim without prejudice to or disclaimer of the subject matter therein, thereby rendering this rejection moot.

Regarding claims 11-18, 32, 43, 44 and 52, Applicants respectfully traverse these rejections. Independent claim 11 recites:

> A computer implemented method for securing a file, the method comprising:
> maintaining a file key in a temporary memory space;
> encrypting the file with the file key in a cipher module to produce an encrypted portion;
> preparing security information for the encrypted portion, the security information being encrypted with a user key and including the file key and access rules to control access to the encrypted portion, wherein the access rules in the security information comprise ***user information identifying*** who has access to the encrypted portion and ***how the encrypted portion is to be accessed***; and
> attaching the security information to the encrypted portion.

Neither Hirano nor Novak, alone or in combination, discloses, teaches, or suggests a method for securing a file that uses user information to identify ***how*** an encrypted portion of a file is to be accessed. Therefore, independent claim 11 is patentable over Hirano in view of Novak.

Furthermore, because each of claims 12-18, 32, 43, 44 and 52 depends upon claims 11, 31, or 40 and because of the additional distinctive features of each of claims 12-18, 32, 43, 44 and 52, each of these claims is also patentable over Hirano in view of Novak.

Accordingly, Applicants respectfully request that the Examiner reconsider and remove the rejections of claims 11-18, 32, 43, 44 and 52 under 35 U.S.C. § 103(a).

Conclusion

All of the stated grounds of rejection have been properly traversed or rendered moot. Applicants therefore respectfully request that the Examiner reconsider all presently outstanding rejections and that they be withdrawn. Applicants believe that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment and Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Timothy A. Doyle

Timothy A. Doyle
Attorney for Applicants
Registration No. 51,262

Date: 20 OCT 08

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

865496_1.DOC